Automating Logistics Support via A Wireless and Satellite Infrastructure

Senior Systems Engineer
Pat Summers
ptsummers@west.raytheon.com

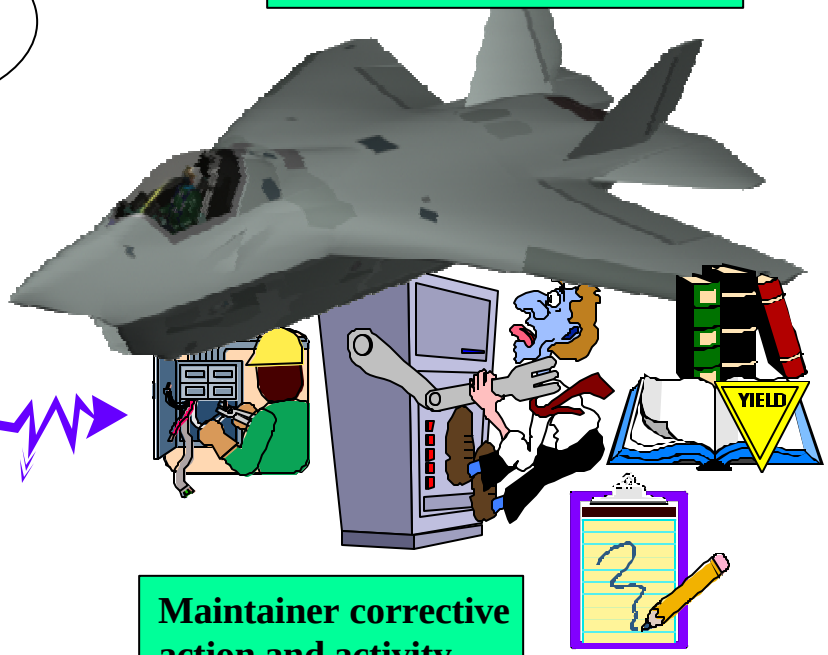
Introduction

- Automating the logistics maintenance process
- Wireless Standards (802.11 and 802.16)
- Using Commercial Satellite links
- Satellite link improvements
- Wireless Security

Current Logistics Maintenance Process

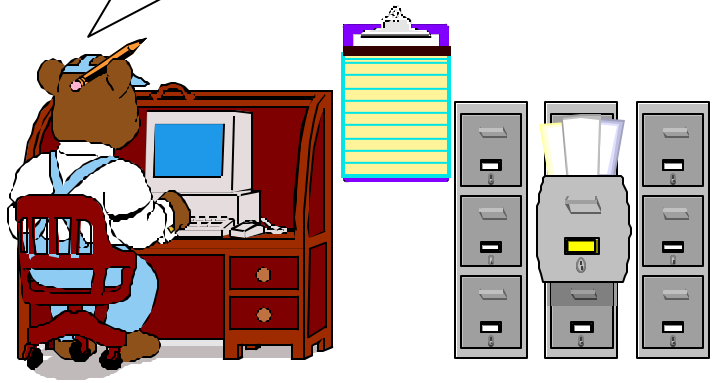
Maintainer Warehouse where maintenance manuals are stored.

Maintainer on Flight line with manuals and spares.



Maintainer corrective action and activity manually logged on paper log sheets.

Where is the space to file these log sheets?



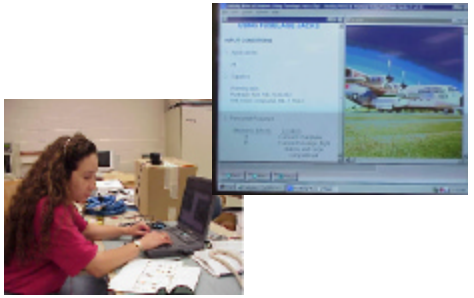
Paper log sheets manually logged in and log sheet is filed.

Automated Maintenance Concept

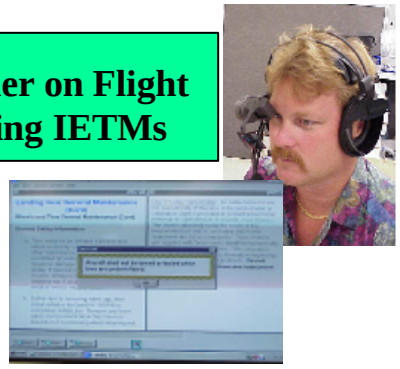
System 2000
PRECISION MAINTENANCE CONCEPT

Raytheon

Maintainer Warehouse Server



Maintainer on Flight line viewing IETMs

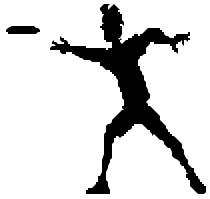


Aircraft Ground Sub-System Integration

"In-flight Aircraft Fault Alerts Sent "

On Demand Maintainer receives wireless information concerning condition of Aircraft

Inter Action



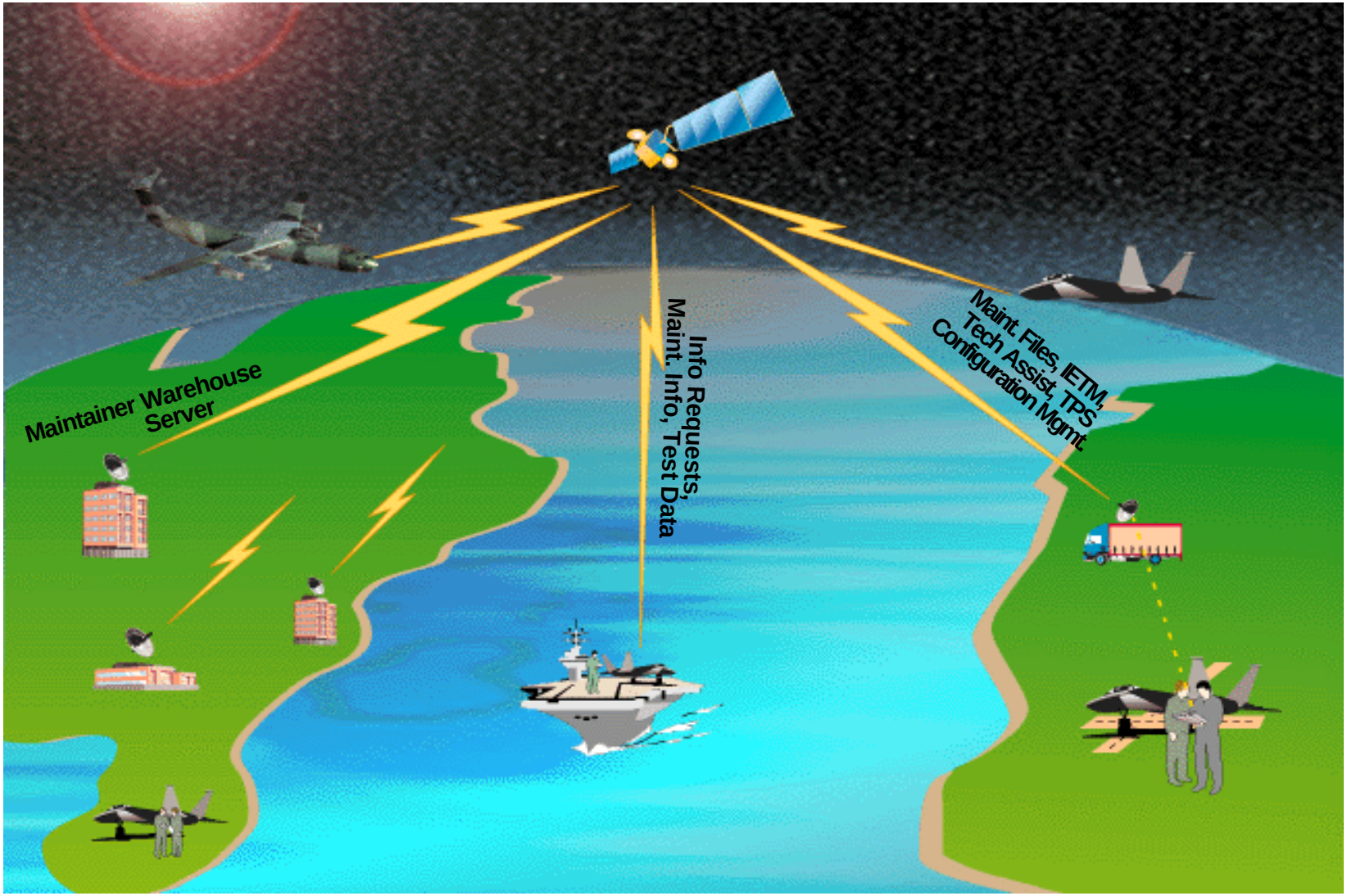
"Maintainer Crew initiate corrective actions"

ALERTS
Notifies Base Supply of Immediate Parts Requirements

Maintainer corrective action and activity automatically logged to Warehouse Server

System 2000

Precision Maintenance Concept

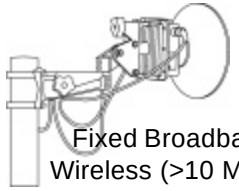


Platform Devices and Infrastructure

Wireless 5.8 GHz Video Link

Direct Broadcast Satellite Receiver

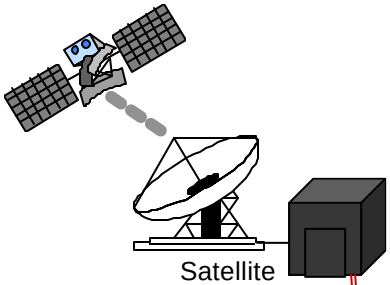
Wireless Phone (cellular, satellite, IP phone, dataphone)



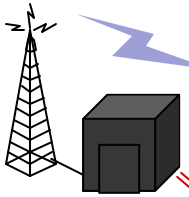
Fixed Broadband Wireless (>10 Mbps)

Digital Assistant

Portable Networking



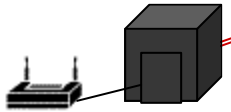
Satellite



Cellular, PCS, Paging, Fixed Wireless

Interconnections may be copper, fiber, coax, or wireless

Public Switched Telephone Network



LAN, SWAN

Ground Communication Technology

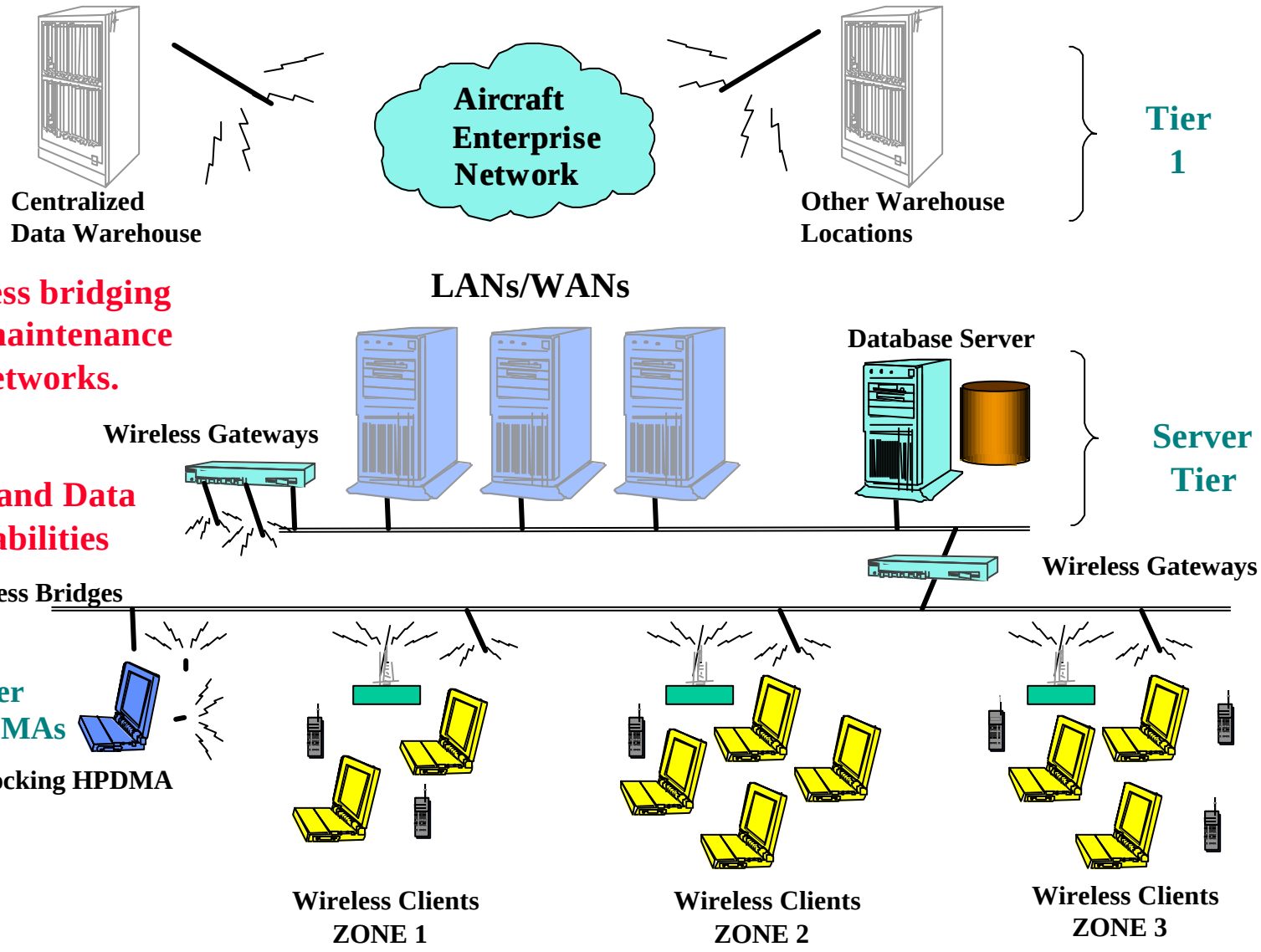
- **Integrated information management through data centric distributed architectures**
- **Planning and decision aids provided for future Business Scenario development**
- **Distributed ground communication architecture to ensure reliable, unambiguous, and accurate information distribution, data timeliness, and data filtering**
- **Integrated wireless technology for seamless architecture**

Wireless Standards

NAME	WHEN PUBLISHED	RANGE/DETAILS
802.11	1997	Operates in a 2.4 GHz range, same as cordless phones
802.11b	1999	Operates in a 2.4 GHz range. This is the standard used by most corporate wireless LANs today. Offers data rates of up to 11 Mbps.
802.11a	1999	Operates in a 5 GHz range. Offers less distance capability between base station and client(s). Proposes to offer data rates of up to 54 Mbps.
802.11e	In development	Will provide enhanced voice transmission and enhanced security features such as larger encryption keys and 128-bit encryption.
802.11g	In development	Operates in a 2.4 GHz range.
802.16.1	In development	Defines the air interface for 10 to 66-GHz systems
802.16.2	In development	Covers coexistence of broadband wireless access systems (such as voice and ATM)
802.16.3	In development	Defines the air interface for licensed systems operating in the 2 to 11-GHz band defines the repeater and reflector interfaces to wireless systems)

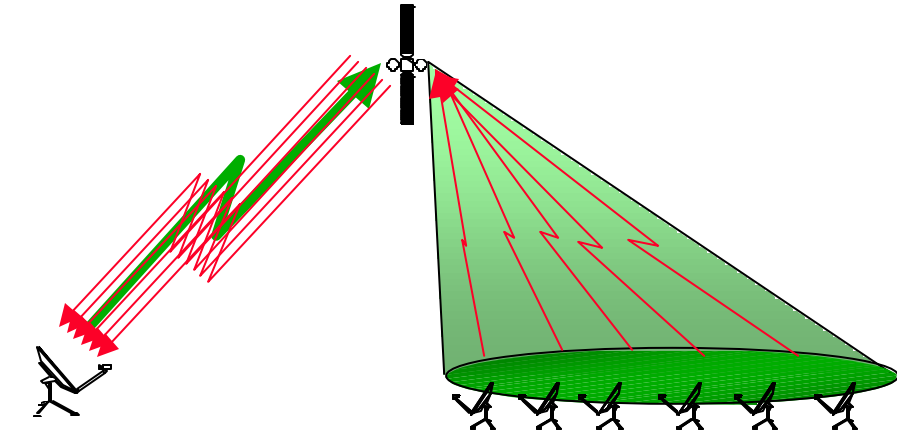
Note: 802.16.x specification data extracted from: "Communication Systems Design (September, 2001), pages 38-46.

Typical Communication Network

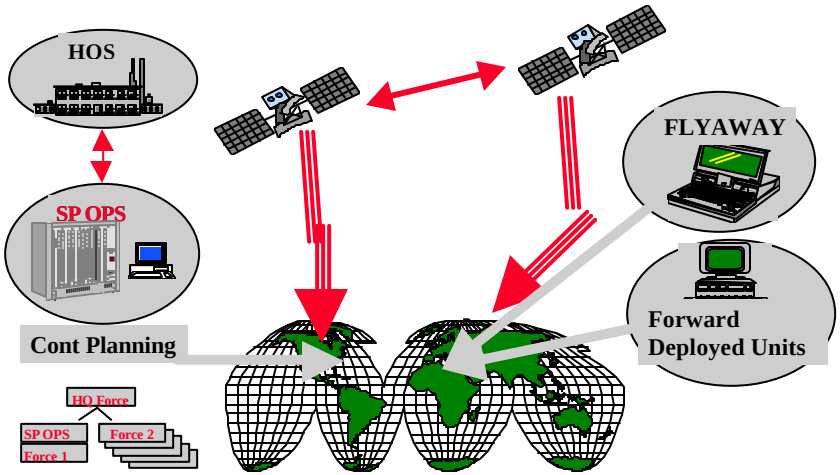


Deployment Options

- **Deployable C4I Satellite System**
  - Commercial off-the-shelf (COTS) Hardware/Software
  - Advanced Integrated Maintenance Support System
- DII-COE Complaint Applications
  - Interoperable with Logistics Operations & Data Bases
  - Rolling Baseline ensures conformity
- Communications
  - Intra/Inter Theater Operations
  - Split based operations, Quickly Deployed
  - Multi-Channel access and Data Integrity
- **Value Added to C2 Operations**
  - Precise logistic status, Just in Time Resupply
  - Improves weapon system and equipment availability
  - Reduces spares in FWD deployed unit
- Eliminates Paper Technical Manuals
- Real Time Logistics support with the Maintainer in the Loop
- Deployable Small VSAT's and Workstations
- Minimal Risk in Wartime
- Leave Behind Capability



Server/HUB



"Real-Time" Satellite Link

- Satellite Link Capable of Utilizing Combinations of Constellations
- Connects to Centralized Data Warehouse
- Uses Small Commercial Low-Cost Portable Dish Antenna and Local File Server
- Wide-Band, Multi-Channel Service Ensures Access-Data Integrity
- Minimal Risk in Wartime
- Examples: GPS, MILSTAR, DSP
- Deployed Theater
- Supports RF Downlinks
- Downloads
  - Test Procedures
  - Maintenance History
  - Interactive Electronic Technical Orders/Manuals (IETMs)
  - C^3 Back-Up, Supply Management, Interactive Training, Medical Consults, Moral Communications
- Redundant, Fail-Safe Performance
- Allows for 24 / 7, Real-Time Support from Conus-Based Cadre (Can Be Distributed) of Technical Experts

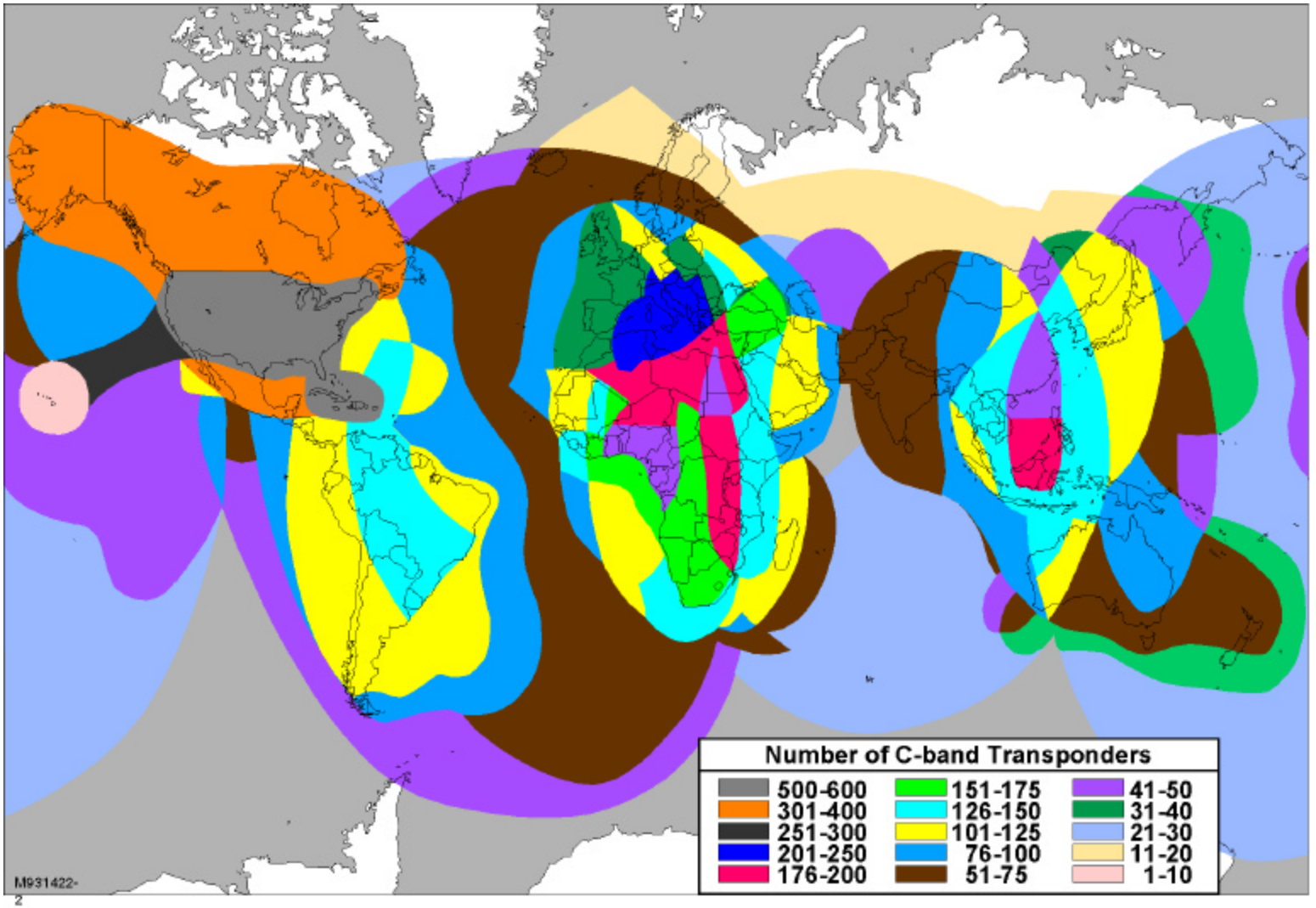
Communication Requirements

- All Communications Channels Are Conditioned to Common CCITT Standards
- Standard EIA-530 Are Used for Modem Interfaces with Cryptographic and Data Processing Equipment
- Data Modems Have Fallback Capabilities During Link Degradation
- Video Links Are Standard CCITT
- Links Will Support both Simplex and Duplex Communications
- Satellite Links Are Reconfigurable by a Dedicated Operations Control Center
- Links Are Protected from RF Power Loads by Automatic Transponders Shutdown
- All Customers Are Ensured a 95% First-Time Success Rate and Link Availability of 99.9%

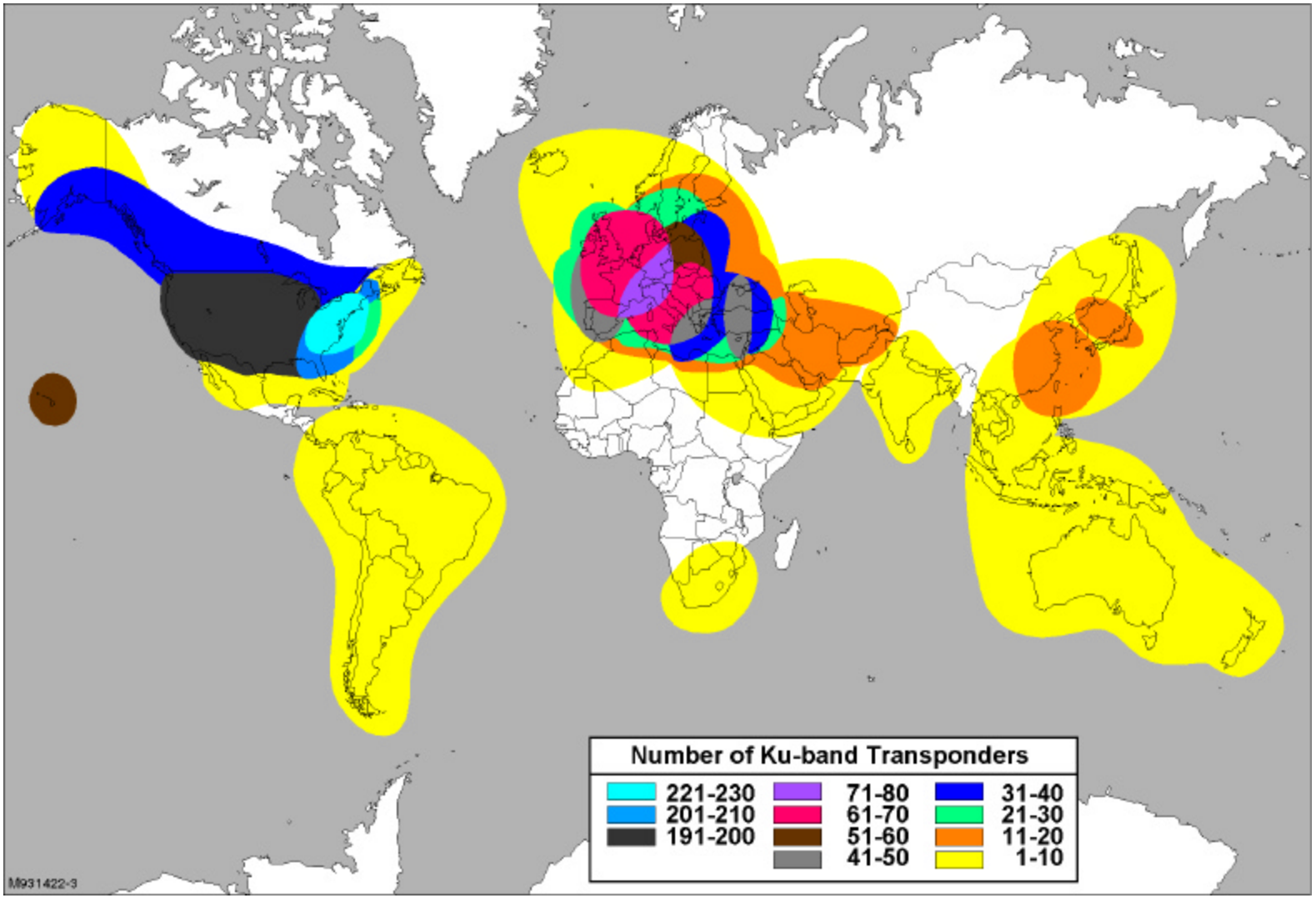
Communication Characteristics

- Ku-Band Frequency Spectrum 11 to 15 GHz
- Ku-Band Transmit Power 4 to 25 Watts
- Wireless Ethernet 2.5 GHz to 5 GHz
- Ethernet Transmit Power 1 Watt – Spread Spectrum
- Antenna Sizes and Mounts
- Satellite Modem
  - QPSK Coding
  - Standard 70 MHz IF Interface
  - Data Rates 2.4 Kbps to 8 Megabits
- Ka-Band Frequency Spectrum 2.5 to 3.5 GHz
- Ka-Band uses smaller antennas so limited to covering smaller areas with spot beams
- Ka-Band is environmentally friendly and more reliable

C-Band Satellite Coverage



Ku-Band Satellite Coverage



Security Scope

- **Security Addresses:**
  - **Confidentiality: prevention of compromise of sensitive/classified data**
  - **Integrity: prevention of unauthorized modification of data**
  - **Availability: prevention of “denial of service” attacks, ensuring availability of critical system services**
- **In a distributed system, we are concerned with security at the following levels:**
  - **Users**
  - **Network security**
  - **Computer Security**
  - **Transmission Security & Encryption**
  - **Application of security technologies in conjunction with OPSEC & Physical security**

Security Techniques

- Identification/Authentication: users, nodes & applications
- Non-repudiation
- Encryption (accomplishes more than confidentiality)
- Intrusion Detection
- Node security (multilevel security, compartmented mode workstations, enclave architectures, application security)
- Wide range of techniques to ensure security functionality within and among network components:
  - Filters, Firewalls, Guards
  - Security Management tools
  - Netlock Management tools

Platform Security Issues

- **Threat Environment**
  - **Three Types**
    - **Connection to the internet, SIPRNET and NIPRNET**
    - **Unauthorized users within the maintenance centralized data warehouse**
    - **Unauthorized user outside of the maintenance centralized data warehouse**
  - **Security Architecture**
    - **Clients are established at the points to be protected**
    - **Reinforced with a USN/USMC specific** behavior model **that will trigger a state transition when an intruder is detected.**
      - This behavior model would capture such information as an intruder mimicking a platoon leader attempting to access a ship database as opposed to a CD-ROM containing a NIPS database file on a landing zone
    - **For virus protection, a Symantec type software may be used**

Encryption Algorithms

- The IEEE 802.11 standard specifies a method called Wired Equivalent Privacy (WEP)
  - –designated RC4, encrypts the message with a 40-bit security key
  - with a higher standard 128-bit key which also may be compromised
  - (Additional WEP security protection is required)
- Netlock implements the IETF IP Security (IPSec) for the TCP/IP and the IPX/SPX protocols
- Kerberos File Key Security from Symbol Technologies
  (Secure data with 128-bit encryption)
- Fortezza Missi
- DES
- For protecting sensitive data in US government voice and data networks, the National Security Agency (NSA) controls which algorithms are exportable outside the US

Anti – Jamming

- Multiple Access
  - —(CDMA)Code division multiple access provides for multiple users Access
- Processing Gain
  - —Protection against interfering signals with finite power provided by spreading of the desired narrowband signal.
- FHSS inherently high security as it hops between 79 channels 2.4-2.4835 GHz at a periodicity random access
  - Therefore, FHSS spectrum jamming is only accomplished by full spectrum interference

Anti - Jamming

- **Short Transmission Range**
  - **Max transmission range is typically limited to 1500 - 3000 ft.**
    - **The transmitted signal is difficult to detect beyond this point.** Maximum power level is 100mW
- **Interference Rejection Properties**
  - **Low Probability of Intercept**
    - **Low power spectral density of spread spectrum makes** information signal noise-like **to unintended users. Jammer has difficulty detecting signal power in the noise-like spectrum.**
  - **Inherent resistance to jamming and interference**
    - **Receiver correlation processing** spreads **the jammer noise over the receiver input bandwidth, while** maximizing **the narrowband signal power. Code correlation receiver** eliminates **multipath interference.**

Summary

- Wireless links improve logistics maintenance efficiency by:
  - Saving Time
  - Reducing people requirements
  - Reducing false removals of system components
  - Reducing spares costs
  - Automating the paper process
  - Can be applied to many existing systems with No or Minimal hardware changes.
- Satellite links reliability and performance are improving
- Wireless technology is constantly evolving - new standards
- Wireless security must be addressed on several levels